

Optimal Discrimination of Qubit States - Methods, Solutions, and Encoder's Freedom

Joonwoo Bae^{1,*} and Won-Young Hwang²

¹Center for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543 and, ICFO-Institut de Ciències Fotòniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain,

²Department of Physics Education, Chonnam National University, Gwangju 500-757, Korea

(Dated: March 2, 2013)

We show a geometric formulation for qubit state discrimination, that can be generally applied, and provide the complete solution in a closed form when arbitrary qubit states are given with equal *a priori* probabilities. It is shown that the guessing probability does not depend on detailed relations among given states, such as angles between them, but on a property that can be assigned by the set of given states itself. This also shows how a set of quantum states can be modified such that they give the same guessing probability. The general structure of optimal measurements is characterized, which also explains that no measurement sometimes gives an optimal strategy.

PACS numbers: 03.65.Ud, 03.67.Hk, 03.65.Wj

Discrimination of quantum states is a fundamental processing to extract information encrypted in collected quantum states. In practical applications, its framework characterizes communication capabilities of encoding and decoding messages via quantum states [1] [2]. Its usefulness as a theoretical tool to investigate quantum information theory has also been shown in secure communication [3] or randomness extraction [4].

Despite of much effort so far [5], however, apart from two-state cases [1], the discrimination task is generally put into a numerical procedure [6] and approximated. Otherwise, restricted cases when some specific symmetry is given can be analyzed, e.g. Ref. [7]. In fact, little is known in general about optimal discrimination once an arbitrary set of quantum states is given. Needless to speak about the importance in its own right, the lack of a general method for state discrimination even in simple instances is, due to its fundamental importance, obviously and also potentially a significant obstacle preventing further investigation in both quantum information theory and quantum foundation.

The present work makes remarkable development in the problem of state discrimination, in particular, for cases of qubit states, and leads to significant improvement along the line. We analyze optimality conditions of the minimum-error discrimination, and provide a geometric formulation of optimal discrimination of qubit states. We show the guessing probability, i.e. the maximal probability of making correct guesses, in a closed form when they are given with equal *a priori* probabilities, and present a method of finding optimal discrimination using the geometry of qubit states. Optimal measurements are characterized accordingly. The discrimination is shown for arbitrary N qubit states in which no symmetry may exist. From these, it is shown that the guessing probability does not depend on detailed re-

lations among given states in general but the property assigned by the set of given states. This shows how a set of states can be modified such that the modification cannot be recognized in the discrimination task.

For the purpose, let us briefly summarize the minimum-error discrimination in the context of a communication scenario of two parties, Alice and Bob. They have agreed with N alphabets $\{x\}_{x=1}^N$ and states $\{\rho_x\}_{x=1}^N$, as well as *a priori* probabilities $\{q_x\}_{x=1}^N$. Alice's encoding works by mapping alphabet x to state ρ_x , and relating states with *a priori* probabilities $\{q_x\}_{x=1}^N$. This can be seen as Alice's pressing button x with probability q_x , and then Bob's guessing among states $\{\rho_x\}_{x=1}^N$ given with *a priori* probabilities $\{q_x\}_{x=1}^N$, which we write by $\{q_x, \rho_x\}_{x=1}^N$.

Bob's discrimination of quantum states is described by Positive-Operator-Valued-Measure (POVM) elements: $\{M_x \geq 0\}_{x=1}^N$ satisfying $\sum_x M_x = I$. Let $P_{B|A}(x|y)$ denote the probability that Bob has a detection event on M_x that leads to the conclusion that ρ_x is given, while a state ρ_y is provided by Alice's sending message y . This is computed as follows, $P_{B|A}(x|y) := P(x|y) = \text{tr}[M_x \rho_y]$. The figure of merit is the maximal probability that Bob makes a correct guess on average, called *the guessing probability*,

$$P_{\text{guess}} = \max_{\{M_x\}_{x=1}^N} \sum_x q_x \text{tr}[M_x \rho_x], \quad \sum_x M_x = I, \quad (1)$$

where the maximization runs over all POVM elements. This naturally introduces the discrimination as an optimization task.

In fact, the above can be put into the framework of semidefinite programming [6]. A useful property in this approach is that a given maximization (minimization) problem can be alternatively described by its dual, a minimization (maximization) problem. The dual problem to the maximization in Eq. (1) is obtained as follows,

$$P_{\text{guess}} = \min_K \text{tr}[K], \quad K \geq q_x \rho_x, \quad \forall x = 1, \dots, N. \quad (2)$$

* bae.joonwoo@gmail.com

In this case, the minimization works to find a single parameter K which then gives the guessing probability, e.g. the approach in Ref. [8].

For convenience, we call the problem in Eq. (1) as the primal, with respect to the dual in Eq. (2). Note that solutions of two problems do not coincide in general. The fact that the guessing probability can be obtained from both primal and dual optimizations follows from the property called strong duality. This holds when both primal and dual problems have a non-empty set of parameters satisfying given constraints, which is referred to as the feasible problems. Once both problems are feasible, the strong duality holds, and then it follows that solutions from both problems coincide each other.

Apart from solving those optimization problems, there is another approach called a *complementarity problem*. This collects optimality conditions that parameters of both primal and dual problems have to satisfy to give optimal solutions. Then, any set of parameters satisfying optimality conditions immediately provide optimal solutions of primal and dual problems. As more parameters are taken into account, this is not considered to be easier, however, the advantage lies at its usefulness to find general structures of a given optimization problem.

In the semidefinite programming formulation, the optimality conditions can be summarized by the so-called Karus-Khun-Tucker (KKT) conditions. For quantum state discrimination, they are given by, together with two constraints in Eqs. (1) and (2),

$$K = q_x \rho_x + r_x \sigma_x, \text{ and} \quad (3)$$

$$r_x \text{tr}[\sigma_x M_x] = 0, \quad \forall x = 1, \dots, N \quad (4)$$

for a set of complementary states $\{\sigma_x\}_{x=1}^N$ with non-negative coefficients $\{r_x \geq 0\}_{x=1}^N$ and POVM elements $\{M_x\}_{x=1}^N$. Once states $\{r_x, \sigma_x\}_{x=1}^N$ and measurements satisfying these conditions are found, they are automatically optimal to give solutions in both primal and dual problems. From the fact that the strong duality holds in this case, it is clear that the guessing probability is obtained from either problem. Note that the former condition in Eq. (3) is called the Lagrangian stability, and shows the existence of a single operator K that can be decomposed into N different ways. The latter one in Eq. (4) is the complementary slackness that shows the orthogonality relation between primal and dual parameters.

The particular usefulness of KKT conditions in state discrimination is that, as it is shown in the above, they separate the guessing probability (i.e. $\text{tr}[K]$ see Eq. (2)) from optimal measurements: a single operator K solely characterizes the guessing probability and optimal measurements itself are independently expressed. The operator K can be explained to have N decompositions of $q_x \rho_x$ and $r_x \sigma_x$ for each x . Optimal measurements can be described as POVM elements orthogonal to states $\{\sigma_x\}_{x=1}^N$

for each x . The discrimination problem is then equivalent to finding states $\{\sigma_x\}_{x=1}^N$ to fulfill these conditions.

We now show a geometric formulation to find complementary states. Let us first define the polytope of given states $\{q_x, \rho_x\}_{x=1}^N$ denoted as $\mathcal{P}(\{q_x, \rho_x\}_{x=1}^N)$ in the underlying state space, in which each vertex corresponds to $q_x \rho_x$. It is useful to rewrite the condition in Eq. (3) as,

$$q_x \rho_x - q_y \rho_y = r_y \sigma_y - r_x \rho_x, \quad \forall x, y \quad (5)$$

This shows that two polytopes $\mathcal{P}(\{q_x, \rho_x\}_{x=1}^N)$ of given states and $\mathcal{P}(\{r_x, \sigma_x\}_{x=1}^N)$ of complementary states to search for are actually congruent. Thus, the structure of complementary states is already determined from given states $\{q_x, \rho_x\}_{x=1}^N$. Once the state geometry is clear e.g. [9], the formulation can be applied.

For qubit states, their geometry can generally be described in the Bloch sphere using the distance measure, Hilbert-Schmidt norm. In what follows, we restrict our consideration to qubit states and apply the geometric formulation to discrimination among them. For a qubit state ρ_x , we write its Bloch vector as $v(\rho_x)$, so that $\rho_x = (I + v(\rho_x) \cdot \vec{\sigma})/2$ where $\vec{\sigma} = (X, Y, Z)$ Pauli matrices X, Y , and Z .

For qubit states, we can characterize the general form of optimal measurements from the KKT condition in Eq. (4). Suppose that $r_x > 0$, otherwise, the measurement can be arbitrarily chosen. To fulfill the condition, it is not difficult to see that optimal POVM elements are either of rank-one [10] or the null operator. If $\sigma_x = |\psi_x\rangle\langle\psi_x|$ then $M_x = m_x |\psi_x^\perp\rangle\langle\psi_x^\perp|$ with coefficients m_x , where it holds that $v(\psi_x) = -v(\psi_x^\perp)$. If a state σ_x is not of rank-one, the only possibility to fulfill the KKT condition in Eq. (4) is that the measurement corresponds to the null operator, i.e. $M_x = 0$. In fact, no measurement can sometimes give optimal discrimination [11]. Note that, however, as measurements are done in most cases (otherwise, the completeness of POVM elements in the following is not fulfilled), one does not have to immediately assume that $\{\sigma_x\}_{x=1}^N$ are not of rank-one from the beginning. Then, for cases where measurements are done, corresponding complementary states must be of rank-one - otherwise, the orthogonality in Eq. (4) cannot be fulfilled.

Once states $\{\sigma_x\}_{x=1}^N$ are found, projectors for optimal measurement are determined accordingly. What remains is that POVM elements fulfill the completeness, $\sum_x M_x = I$, or equivalently in terms of Bloch vectors, $\sum_x m_x v(\psi_x^\perp) = 0$ while $\sum_x m_x = 2$ with $m_x \geq 0, \forall x$. This refers to finding a convex combination $\{m_x\}_{x=1}^N$ of Bloch vectors $\{v(\psi_x^\perp)\}_{x=1}^N$ such that it results to zero, i.e. the origin of the Bloch sphere. This is equivalent to the condition that the convex hull of Bloch vectors $\{v(\psi_x)\}_{x=1}^N$ of complementary states contain the origin of Bloch sphere. As we will show later, this is always fulfilled by complementary states. To summarize, once complementary states are found, it is automatic to have

optimal POVMs as their Bloch vectors are determined and the completeness is also straightforward.

We can thus proceed to construction of complementary states in the Bloch sphere for qubit states $\{q_x, \rho_x\}_{x=1}^N$. Let us identify the polytope $\mathcal{P}(\{q_x, \rho_x\}_{x=1}^N)$ in the state space as the convex hull of their Bloch vectors $\{q_x, v(\rho_x)\}_{x=1}^N$, so that each vertex $q_x \rho_x$ corresponds to the Bloch vector $q_x v(\rho_x)$. Then, the task is to find the polytope $\mathcal{P}(\{r_x, \sigma_x\}_{x=1}^N)$ of complementary states that is congruent to $\mathcal{P}(\{q_x, \rho_x\}_{x=1}^N)$ in the Bloch sphere. Moreover, as it is shown, most of complementary states $\{\sigma_x\}_{x=1}^N$ are of rank-one and themselves lie at the border, thus, the polytope $\mathcal{P}(\{\sigma_x\}_{x=1}^N)$ only of them is maximal in the Bloch sphere. Using these, a geometric approach can be generally employed.

All these already give the guessing probability in a simple way for cases when qubit states are given with equal *a priori* probabilities, that is, when $q_x = 1/N$ for all x . In this case, it is not difficult to see a general form of the guessing probability. Substituting $q_x = 1/N$ in the KKT condition in Eq. (3), it is obtained that parameters $\{r_x\}_{x=1}^N$ are equal. We put $r := r_x$ for all x . This holds true for arbitrary set of quantum states in general. Then, the guessing probability is written as

$$P_{\text{guess}} = \text{tr}[K] = \frac{1}{N} + r, \text{ with } r = \frac{\|\frac{1}{N}\rho_x - \frac{1}{N}\rho_y\|}{\|\sigma_x - \sigma_y\|}, \quad (6)$$

where the equation for the parameter r is from the relation in Eq. (5), and the distance measure can be taken as the Hilbert-Schmidt norm D_{HS} (as it is natural in the Bloch sphere) or the trace norm D_T . Both measures give the same value of r since they are related only by a constant: $D_{\text{HS}} = \sqrt{2}D_T$ for qubit states. This means that, the parameter r can be obtained by either of distance measures while referring to the geometry in the Bloch sphere, since the parameter is only a ratio, see Eq. (6).

The parameter r corresponds to the ratio between two polytopes, $\mathcal{P}(\{1/N, \rho_x\}_{x=1}^N)$ of given states and the other $\mathcal{P}(\{\sigma_x\}_{x=1}^N)$ only of complementary states, as it is shown in Eq. (6). We recall that most of $\{\sigma_x\}_{x=1}^N$ are pure (i.e. rank-one), lying at the border of the Bloch sphere. This implies that the polytope $\mathcal{P}(\{\sigma_x\}_{x=1}^N)$ of complementary states is clearly the maximal in the Bloch sphere. In this way, the polytope $\mathcal{P}(\{\sigma_x\}_{x=1}^N)$ always contain the origin of the sphere, from which optimal measurements can be constructed. Finally, two polytopes $\mathcal{P}(\{1/N, \rho_x\}_{x=1}^N)$ and $\mathcal{P}(\{\sigma_x\}_{x=1}^N)$ are similar from the relation in Eq. (5) by the ratio r , since two polytopes $\mathcal{P}(\{1/N, \rho_x\}_{x=1}^N)$ and $\mathcal{P}(\{1/N, \sigma_x\}_{x=1}^N)$ are congruent.

We summarize the method of discrimination.

- 1: Construct a polytope from given states as the convex hull of $\{1/N, v(\rho_x)\}_{x=1}^N$ in the Bloch sphere where vertices are $v(\rho_x)/N$.
- 2: Expand the polytope such that it keeps similar to the original one and is also maximal in the Bloch sphere

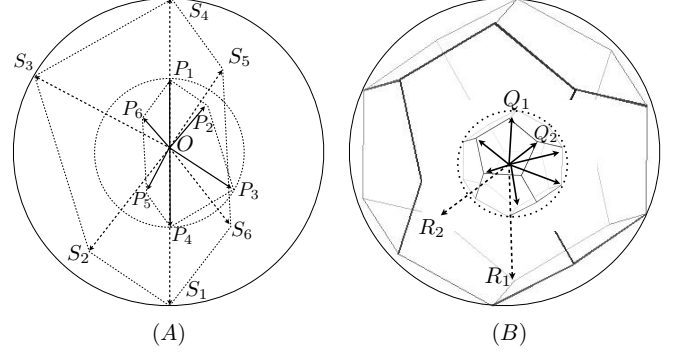


FIG. 1. (A) Six states $\{1/6, \rho_x\}_{x=1}^6$ in the half-plane are given with purities $\{f_x\}_{x=1}^6$, i.e., $OP_x = f_x/6$, where three of them ($x = 1, 3, 4$) have the same purity and the others are less. See also that the relation in Eq. (5) is fulfilled. The ratio r in Eq. (6) can be obtained by expanding the given polytope until it is maximal in the plane. This is also the ratio between radii of two circles covering respective polygons. Thus, $P_{\text{guess}} = 1/6 + f_1/6$. Complementary state σ_x corresponds to OS_x . For $x = 2, 5, 6$, they are not pure states and thus no measurement on these states is optimal [10]. (B) For $\{1/N, \rho_x\}_{x=1}^N$ of pure states, each vertex of the polyhedron corresponds to the Bloch vector of state ρ_x/N . The ratio r is equal to Q_1Q_2/R_1R_2 , see also Eq. (5), and thus $P_{\text{guess}} = 2/N$. Even if these states are modified, if the minimal sphere covering the polyhedron is unchanged, the guessing probability remains the same.

(as most of $\{\sigma_x\}_{x=1}^N$ are pure), and then compute the ratio r of the resulting polytope with respect to the original one. The guessing probability is thus obtained, $P_{\text{guess}} = 1/N + r$.

- 3: Rotate the maximal polytope within the Bloch sphere until it is found that corresponding lines are parallel to the original ones to fulfill Eq. (5). From this, corresponding vertices are complementary states $\{\sigma_x\}_{x=1}^N$ and optimal POVM elements are explicitly constructed accordingly.

This completely solves the problem of discrimination of qubit states given with equal *a priori* probabilities.

It is already observed that the guessing probability does not depend on detailed relations of given quantum states to discriminate among, but a property from the whole set $\{\rho_x\}_{x=1}^N$, since its ratio r is the relevant parameter. If given states are modified such that the polytope has the same ratio r , then the same guessing probability is given. This means that, in the communication scenario we have introduced in the beginning, Alice who encodes messages can choose, or modify, sets of quantum states $\{\rho_x\}_{x=1}^N$ in such a way that Bob who decodes from quantum states cannot recognize her modification using the optimal guessing. This actually defines equivalence classes of sets of quantum states in terms of optimal

guessing [12].

In the following, we apply the method to various cases of qubit state discrimination. The simplest example, also the case when a general solution is known, is for $N = 2$, say ρ_1 and ρ_2 . Following the instruction in the above, i) the polytope constructed by given two states corresponds to a line connecting two Bloch vectors of the states. The length can be computed using the trace distance as $\|\rho_1 - \rho_2\|/2$. Then, ii) the maximal polytope similar to the original one is clearly the diameter of the Bloch sphere, which has length 2 in terms of the trace distance, hence, $r = \|\rho_1 - \rho_2\|/4$ (which equivalently can be obtained with the Hilbert-Schmidt distance). Substituting this in Eq. (6), the Helstrom bound in Ref. [1] is reproduced. Then, iii) the diameter can be rotated until it is parallel to the original one. Thus, optimal measurements are also obtained.

Next, let us consider N states on the half-plane. We can begin with those states $\{1/N, \rho_x\}_{x=1}^N$ which are equally distributed and generally not pure. They are characterized by Bloch vectors: $\mathbf{v}(\rho_x) = f_x(\cos \theta_x, \sin \theta_x, 0)$ where $\theta_x = 2\pi x/N$. For these, no general solution is known except cases called geometrically uniform states, that $\{f_x\}_{x=1}^N$ are equal [7]. Here, suppose that N is even so that we can also assume $f_{N/2} = f_N = \max_x f_x$. Then, applying the method introduced, one can easily find that the ratio depends on the maximal purity, that is, $r = f_N/N$, and the guessing probability is obtained as $P_{\text{guess}} = 1/N + f_N/N$, no matter what purities the other $N-2$ states have, see also Fig. 1. The result in Ref. [7] is also reproduced. The assumption of the equal distribution on angles can be relaxed while keeping $\theta_N = \pi + \theta_{N/2}$ and $f_{N/2} = f_N = \max_x f_x$, for which the guessing probability is also the same no matter how other $N-2$ states are structured. This is because, as it is shown in Eq. (6), they are given with equal probabilities and the ratio r is unchanged.

Optimal measurements can be analyzed as follows, based on the geometric formulation, see also Fig. 1. For two states $\rho_{N/2}$ and ρ_N having the maximal purity, it is clear that measurement is applied, and let $\sigma_N = |\psi_N\rangle\langle\psi_N|$ and $\sigma_{N/2} = |\psi_{N/2}\rangle\langle\psi_{N/2}|$. From these, optimal POVM elements are straightforward. For the other states, say $\{\rho_z\}$ having $f_z < f_N$, it holds from the KKT condition in Eq. (5) that $\mathbf{v}_N - \mathbf{v}_z$ is parallel to $r(\mathbf{v}(\sigma_N) - \mathbf{v}(\sigma_z))$. This simply shows that their complementary states $\{\sigma_z\}$ cannot be pure states, i.e. not of rank-one. Then, corresponding POVM element is the null operator, that is, no measurement on these states gives an optimal strategy.

The method can be applied to a set of qubit states having a volume. For instance, let us look at the case when pure states are given such that their Bloch vectors form a regular polyhedron of N vertices, see Fig. 1. Following the instruction in the above, the parameter r can be obtained as the ratio of two spheres, one

the Bloch sphere and the other the minimal sphere covering the polyhedron of given states $\{1/N, \rho_x\}_{x=1}^N$. From this, we have $r = 1/N$, and the guessing probability is thus, $P_{\text{guess}} = 2/N$. One can also modify angles between those N states such that the minimal sphere covering the polyhedron remains the same, and then the guessing probability is unchanged.

The presented method can be in principle applied to, high dimensional states once their geometry is clear, or qubit states with unequal *a priori* probabilities. For the latter, although the geometry is clear, we do not have yet a general and systematic method to derive the guessing probability. For these cases, interesting and illuminating examples are to be presented elsewhere [12].

To conclude, we have shown a geometric formulation for qubit state discrimination and provide the guessing probability in a closed form for equal *a priori* probabilities. This makes a significant contribution to the study of quantum state discrimination. Optimal measurements are characterized accordingly. It is shown how qubit states can be modified while the guessing probability remains the same. As qubits are units of quantum information processing, we envisage that the method of discrimination and results presented here would be useful to develop further investigations of qubit applications, or approaches to related open questions e.g. Ref. [13].

This work is supported by National Research Foundation and Ministry of Education, Singapore, and Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2010-0007208).

-
- [1] C. Helstrom, Quantum Detection and Estimation Theory Academic, New York, ADDRESS, (1976).
 - [2] Y. C. Eldar and A. V. Oppenheim, Signal Processing Mag., vol. **19**, pp. 12-32, Nov. 2002.
 - [3] R. Koenig, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theory, **55**, 9 (2009).
 - [4] S. Pironio, A. Acín, S. Massar *et. al.*, Nature **464**, 1021 (2010).
 - [5] A. Chefles, Contemporary Physics **41**, 401 (2000); J. A. Bergou, U. Herzog, and M. Hillery, Lect. Notes Phys. 649, 417-465 (Springer, Berlin, 2004); J. A. Bergou, J. Phys: Conf. Ser. **84**, 012001 (2007); S. M. Barnett and S. Croke, Adv. Opt. Photon. **1**, 238278 (2009); J. A. Bergou, Journal of Modern Optics, Vol. **57**, Issue 3, 160-180 (2010).
 - [6] S. Boyd and L. Vandenberghe, Convex Optimization, Cambridge University Press, (2004).
 - [7] Y. C. Eldar and G. D. Forney, IEEE Trans. Inf. Theory **47**, 3 (2001).
 - [8] M. E. Deconinck and B. M. Terhal, Phys. Rev. A **81**, 062304 (2010).
 - [9] I. Bengtsson and K. Życzkowski, Geometry of Quantum States, Cambridge University Press (2006).
 - [10] The only possibility to choose a positive operator σ_x such

that $\text{tr}[\sigma_x M_x] = 0$ for a positive operator M_x of rank-two is that $\sigma_x = 0$. This is taken into account in the the case when $r_x = 0$ in the KKT conditions, and therefore excluded. Then, POVM elements are either rank-one or

the null operator.

[11] K. Hunter, Phys. Rev. A **68**, 012306 (2003).

[12] J Bae, in preparation.

[13] Prob.31 in <http://qig.itp.uni-hannover.de/qiproblems>.